REMARKS

The Examiner has finally rejected claims 16 and 17 under 35 U.S.C. 103(a) as being unpatentable over European Patent Application No. EP0752635A1 to Samar. Applicants acknowledge that the Examiner has allowed claims 1-11.

The Samar patent discloses a system and method to transparently integrate private key operations from a smart card with host-based encryption services, in which a computer 101 having a smart card reader 121 and an associated smart card 123 is connectable over a network 115 to a remote computer 119 or a terminal 117 each having a smart card reader 121 and optionally an associated smart card 123. If the user of the computer 101 has a smart card 123 and inserts the same into the reader 121, the computer 101 enables the transmission of messages encrypted in accordance with the contents of the smart card 123. If no smart card is inserted, the computer 101 enables the transmission of messages encrypted in accordance with the contents of a user information file 127 and encryption services 129.

The subject invention relates to the transmission and reception of encrypted signals in, for example, a cable television system. In particular, at a headend, the cable provider encrypts a first signal in accordance with a first encryption scheme, and encrypts a second signal in accordance with a second encryption scheme. The cable provider then transmits both encrypted first and second signals. This is shown in Fig. 5, and in the specification on page 12, lines 10-13, where it is stated that the transmission

station continually transmits the encrypted first and second signals.

The invention, as claimed in claim 16, discloses encrypted transmissions of at least one signal, the first conditional access module only being able to decrypt a portion of the at least one signal (which may then correspond to a first signal), and the second conditional access module being able to decrypt the whole of the at least one signal (which may then correspond to a second signal). Since the whole of the at least one signal and the portion of the (same) at least one signal is transmitted "at the same time", Applicants submit that the distinguishing features of claim 1 is indeed included in claim 16.

With regard to Samar, the encryption scheme being used to encrypt a signal being sent to the computer already takes into consideration whether or not the computer has a smartcard inserted therein. At no time does Samar disclose or suggest the transmission and reception of a signal in which a first conditional access module is only able to decrypt a portion of the signal, while the second removable conditional access module is able to decrypt the whole of the signal.

Further, Applicants note that in the last Office Action, the Examiner states:

> "Regarding claim 16, Samar teaches "A system for decrypting encrypted transmissions of at least one signal, comprising a receiver for receiving transmissions of the at least one signal, the receiver including a first embedded conditional access module having a decryption algorithm capable of decrypting a portion of the at least one signal and a second

removable conditional access module having a decryption algorithm capable of decrypting the entire at least one signal (column 7, lines 10-51, the system having an access with input), wherein enabling of the second removable conditional access module causes the second removable conditional access module to override the first conditional access module (column 2, line 13 to column 4, line 14, access with smart cards - which would get information from smart card rather than from the regular input)."

These passages of Samar do not teach "module" in the sense of the claim.

Nevertheless, it was well known in the art to have a "module" situation for the motivation of having easier control and handling."

First, Applicants would like to point out that none of these passages are of (from) Samar. Rather, the Examiner has merely reproduced claim 16 and indicated where in Samar the Examiner believes that each limitation is found.

Further, Applicants submit that Samar merely discloses that a user with an appropriate smart card is authenticated by the system, while without a smart card "the operating system 135 authenticates 221 the user with any of the selected encryption services 129." Once authenticated, the user, whether or not a smart card is present, is allowed onto the system. Applicants submit that there is no disclosure in Samar of "the receiver including a first embedded conditional access module having a decryption algorithm capable of decrypting a portion of the at least one signal and a second removable conditional access module having a decryption algorithm capable of decrypting the entire at least one signal".

In view of the above, Applicants believe that the subject invention, as claimed, is not rendered obvious by the prior art, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-11, 16 and 17, claims 12-15 having been withdrawn, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by /Edward W. Goodman/
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611